

Installation og brug af SSL-certifikater: Sådan gør I det rigtigt





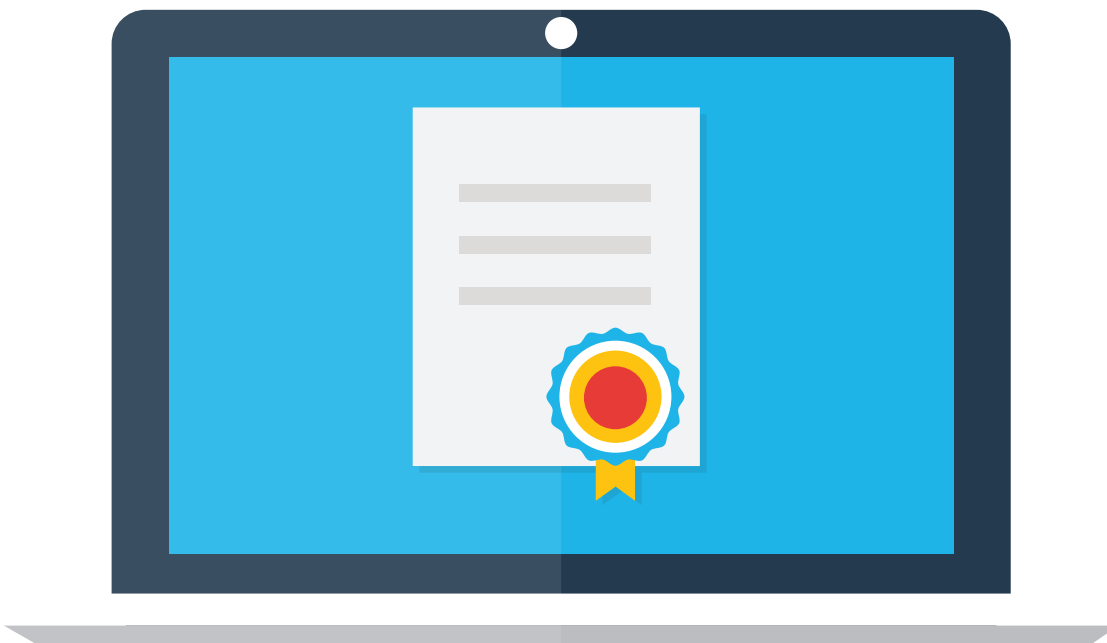
I har købt jeres SSL-certifikat(er), og hvad så nu?

Køb af certifikater er blot det første af en række trin til at beskytte jeres websted. Alt for ofte bliver certifikater ikke installeret rigtigt, datafølsomme sider bliver ikke beskyttet ordentligt, og indtastede oplysninger i formularer bliver ikke krypteret med det resultat, at mange websteder er sårbare over for angreb.

Derfor indeholder denne vejledning fra Symantec en række tip til, hvordan I får jeres certifikat(er) til at fungere helt rigtigt fra starten. Dermed undgår I de største farer, og I bliver advaret mod usikre vaner og fremgangsmåder, som kan underminere SSL, fordi SSL-certifikatet er jeres pas eller kørekort til et sikrere og bedre beskyttet websted for jer, jeres medarbejdere og jeres kunder.

SSL skal installeres på én måde – den rigtige!

Som mange andre firmaer har I fundet ud af, at et SSL-certifikat er nødvendigt, og har taget dette vigtige skridt på grund af sikkerheden. Det næste skridt består i at installere det rigtigt. Hvis kunderne ikke er helt trygge ved sikkerheden på jeres websted, handler de ganske enkelt ikke hos jer.





TIP nr. 1 - Oprettelse af den private nøgle og CSR



For at installere et digitalt certifikat skal I først oprette den private nøgle og anmodningen om certifikatunderskrift (Certificate Signing Request (CSR)) ud fra den private nøgle til den server, hvor certifikatet skal installeres. Derefter skal den oprettede CSR indsendes for at ansøge om et certifikat. Her er fremgangsmåden.

Hvis I har IIS 6-servere eller nyere eller Redhat Linux-servere, kan I downloade vores hjælpeprogram [Symantec SSL Assistant](#) og blot følge den brugervenlige vejledning. Se her for en oversigt over vejledninger til at oprette CSR på andre servere: [Oprettelse af Symantec CSR](#). For at ansøge om Symantecs SSL-certifikatløsninger skal I bruge følgende oplysninger:

- Certifikatets løbetid eller gyldighedsperiode: 1, 2 eller 3 år
- Antallet af servere, der er vært for et enkelt domæne (op til 5 servere)
- Serverplatformen
- Firma, organisationsenhed, adresse
- Betalingsoplysninger og kontaktoplysninger til fakturering
- Fællesnavnet. Det er værtsnavnet + domænenavnet, f.eks. "www.mitdomæne.dk" eller "webmail.mitdomæne.dk"
- En mailadresse, hvor Symantec kan kontakte jer for at bekræfte informationen
- En anmodning om certifikatunderskrift (CSR) oprettet fra serveren, I skal have beskyttet

Når I derefter har fået certifikatet, skal I følge vejledningen under tip nr. 3.

Hvis serveren ikke er på listen, eller hvis I har brug for yderligere oplysninger, skal I se i serverdokumentationen eller kontakte serverleverandøren. Hvis I ikke ved, hvilken software der er på jeres server, skal I kontakte jeres it-administration.

Ved ansøgning skal den oprettede CSR indsendes med denne header og footer:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



TIP nr. 2 - Sådan installeres et SSL-certifikat, på den rigtige måde!



Skal I installere et SSL-certifikat for første gang og synes, at det virker uoverskueligt? Det er det faktisk ikke. Det er meget nemmere, end I tror. Her er overblikket over, hvordan et certifikat installeres på en server, med Symantec.

Den overordnede fremgangsmåde er den samme for alle servere:

Trin 1 – Gem certifikatet på computeren

Følg vejledningen i den bekræftende e-mail for at downloade SSL-certifikatet til din computer fra den oplyste webadresse. Så har I både certifikatet og de mellemliggende CA-certifikater, I skal bruge.

Trin 2 – Installer eller flyt det til en certifikatmappe

Trin 3 – Konfigurer certifikatet på webstedet

Trin 4 – Opret reference til certifikatet

[Klik her](#) for udførlige oplysninger og trinvis vejledning til alle servertyper.

For at få fuldt udbytte af jeres SSL-certifikat skal I sætte Norton Secured-seglet på jeres websted. Det gør jeres kunder mere trygge ved sikkerheden, når de handler hos jer.

I skal blot kopiere og indsætte de relevante linjer fra Symantecs Norton Secured-seglsider for at sætte seglet på jeres websted. Den overskuelige vejledning findes via linket nederst i dette tip. Her kan I også læse, hvordan I tester certifikatet ved hjælp af kontrolfunktionen Certificate Installation Checker ved at indtaste jeres domæne, når I bliver bedt om det.

Nu er SSL-certifikatet installeret – og klar til brug

Problemer?

Symantec har en række instruktionsvideoer til forskellige servere: [Se instruktionsvideoer](#)

Kontroller jeres installation

Indtast webadressen for den server, der skal kontrolleres: [Kontrollér installationen](#)

Opret seglet til jeres websted

Vejledning til installation af Norton Secured-seglet: [Opret seglet](#)

Fejlfinding

Gå ind på Symantecs supportwebsted: [Brug supporten](#)



TIP nr. 3 - Beskyt jeres private nøgler, og få den bedste løsning



Offentlige og private nøgler er en integreret del af funktionaliteten af SSL. Den private nøgle hemmeligholdes på serveren og anvendes til at kryptere alt på webstedet. Den offentlige nøgle, som er inde i certifikatet, er en anden del af jeres websteds identitet, f.eks. jeres domænenavn og firmaoplysninger.

I skal passe på jeres private nøgler, som var de uvurderlige genstande, og kun give det absolut nødvendige antal pålidelige forretningspartnere eller medarbejdere kendskab til dem. Hvis du f.eks. var bankdirektør, ville du så udlevere nøglerne til bankboksen til hvem som helst? Nej, vel. Så her er nogle praktiske tip:

- **Opret private nøgler på en server, der er tillid til.** Overlad ikke dette til andre uden for virksomheden!
- **Beskyt private nøgler med adgangskode** for at undgå kompromittering ved lagring i backupsystemer
- **Forny certifikater hvert år** – og opret altid nye private nøgler ved samme lejlighed.

Længden af den private nøgle har stor indflydelse på det kryptografiske “håndtryk”, der anvendes til at oprette sikre forbindelser. Brug af nøgler, der er for korte, er en usikker praksis, mens nøgler, der er for lange, kan nedsætte systemhastigheden markant.

Elliptic Curve Cryptography (ECC), som vinder stadig større udbredelse, øger sikkerheden ved hjælp af kortere nøglelængder. Symantec leverer ECC med nøglelængder, der indeholder en brøkdel af det antal bits, som RSA og DSA har brug for, og er alligevel mere end 10.000 gange sværere at bryde (256-bit til ECC svarer til den kryptografiske styrke med 3072-bit RSA). ECC giver bedre sikkerhed, belaster servere meget mindre og reducerer antallet af CPU-cykler ved kryptografiske operationer på servere.

Se side 7 for flere oplysninger om ECC.



TIP nr. 4 - Undgå svage led i kæden



I de fleste SSL-installationer er et servercertifikat alene ikke tilstrækkeligt: en ubrudt tillidskæde kræver mindst tre certifikater. En certifikatkæde består af alle de certifikater, som er nødvendige for at bekræfte den, som er navngivet i det sidste certifikat i kæden.

I praksis omfatter denne kæde End Entity-certifikatet, mellemliggende certificeringscentres (CA) certifikater og rodcertificeringscentrets certifikat.

Processen for bekræftelse af ægtheden og gyldigheden af et nyt certifikat, som en kunde har modtaget, omfatter kontrol af alle certifikaterne fra det universelt anerkendte rodcertificeringscenter, lige fra eventuelle mellemliggende CA-certifikater og til det netop modtagne certifikat ("End Entity-certifikat"). Der er kun tillid til et certifikat, hvis hvert certifikat i det pågældende certifikats kæde er udstedt og kontrolleret korrekt.

Et typisk problem er, at End Entity-certifikatet konfigureres korrekt, men at man glemmer at medtage de mellemliggende CA-certifikater. Brug vores [certifikatkontrollfunktion](#) til at kontrollere, at de mellemliggende certifikater er installeret korrekt.



TIP nr. 5 - RSA, ECC, og hvorfor nøglelængden er vigtig



Med Elliptic Curve Cryptography (ECC) får jeres virksomhed forbedret sikkerhed og højere systemhastighed end med nuværende krypteringsmetoder.

ECC er en krypteringsmetode, som er godkendt i USA af staten og af sikkerhedstjenesten NSA, og som opretter krypteringsnøgler baseret på et koncept, der anvender punkter på en elliptisk kurve til at definere det offentlige/private nøglepar. Metoden er vanskelig at bryde ved hjælp af brute force-angreb, som hackere ofte anvender, og det er en hurtigere løsning, som kræver mindre computerkraft end RSA-baseret kryptering.

RSA er en krypterings- og digital signeringsalgoritme, der har været grundlaget for sikkerhed på nettet i snart to årtier. Algoritmen er stadig anvendelig, men den acceptable minimumlængde for nøgler er blevet længere med tiden for at beskytte mod stadigt skrappe kryptografiske angreb. Derfor er systemhastigheden højere med ECC, fordi denne metode fungerer med en kortere nøglelængde, og sikkerheden er ekstra høj. Eksempelvis beskytter en 256-bit ECC-nøgle lige så godt som en RSA-nøgle på 3072 bit. Resultatet er, at I får netop den sikkerhed, I har brug for, uden at gå på kompromis med systemhastigheden.

Samtidig gør de kortere ECC-nøglelængder certifikaterne mindre, så de bruger mindre båndbredde. I takt med at flere af jeres kunder går over til at bruge mindre enheder til at foretage transaktioner på nettet, bliver kundeoplevelsen bedre på alle punkter med ECC.

Symantecs ECC-rødder har været tilgængelige i de tre mest anvendte browsere siden 2007. Derfor fungerer Symantecs ECC-certifikater i jeres nuværende infrastruktur, når brugerne har de nyeste browserversioner, og ECC-rødderne er gratis tilgængelige.

Få mere at vide om [ECC og brug af forskellige algoritmer](#).



TIP nr. 6 - Fuldt omfattende sikkerhed med Always On SSL



I bør altid sørge for, at hele jeres websted er krypteret med SSL. Og måden at gøre det på er med Always On SSL. Det er en omkostningseffektiv sikkerhedsforanstaltning til websteder, som sikrer hele brugeroplevelsen fra start til slut, så brugerne er beskyttet, når de søger, udleverer info og køber på nettet.

Firmaer, der er seriøse med at beskytte deres kunder og virksomhedens omdømme, installerer Always On SSL med SSL-certifikater fra et anerkendt certificeringscenter, som f.eks. Symantec. Always On SSL er nemt at installere, bekræfter webstedets identitet og krypterer al information, der udveksles mellem webstedet og en bruger (inkl. alle cookies), så dataene er beskyttet mod uvedkommende læsning, manipulation eller anvendelse.

Desuden anbefaler en betydningsfuld organisation som Online Trust Alliance, at websteder anvender Always On SSL. Rådet fra denne organisation er, at "Always On SSL er en veletableret, praktisk sikkerhedsforanstaltning, der bør implementeres på alle websteder, hvor brugere udveksler eller læser følsomme oplysninger".

Mange af verdens mest succesrige websteder har indset fordelene og implementeret Always On SSL for at beskytte sig mod sessionskaping og hackerangreb i form af trusler som f.eks. Firesheep og inficering med skadelig kode.

Med Always On SSL kan I opretholde den tillid, som brugerne har til jeres websted, ved at forsikre dem om, at I tager netsikkerhed og beskyttelsen af deres fortrolige oplysninger seriøst, og at I træffer alle tænkelige sikkerhedsforanstaltninger for at beskytte dem på nettet.



TIP nr. 7 - Public Key Pinning: et spørgsmål om tillid



Formålet med Public Key Pinning (den fulde betegnelse er Public Key Pinning Extension til HTTP) er at give webstedsoperatører mulighed for at bestemme, hvilke certificeringscentre der kan udstede certifikater til deres servere.

Public Key Pinning fungerer ved at tilknytte en vært med dennes forventede certifikat eller offentlige nøgle. Når en vært kender eller registrerer en offentlig nøgle, bliver den offentlige nøgle tilknyttet ("pinned" til) denne vært.

Ifølge CA Security Council giver Public Key Pinning webstedsejere mulighed for at forsikre omverdenen om, at et eller flere af følgende aspekter gør sig gældende for deres SSL-certifikat:

- En specifik offentlig nøgle
- Et certificeringscenter har signeret det med denne offentlige nøgle
- Hierarkisk baseret tillid til et certificeringscenter med denne offentlige nøgle

Hvis et certifikat for webstedsejerens domæne er udstedt af et certificeringscenter, der ikke findes på listen (dvs. ikke er "pinned"), bliver der vist en advarsel om manglende tillid i browseren, som understøtter Public Key Pinning. Webstedsejere kan desuden tilknytte flere nøgler fra forskellige certificeringscentre, som alle vil blive accepteret af browserne.

Webstedets ejer har tillid til, at de valgte certificeringscentre ikke kommer til at udstede et certifikat til ejerens domæne ved en fejl. Disse certificeringscentre fører kontrol med, hvem der kan bede om at få udstedt et certifikat til ejerens specifikke domæner: Det sikrer yderligere mod fejlagtig udstedelse af certifikater til uvedkommende.

Desværre, som CA Security Council gør opmærksom på, er den Public Key Pinning, som Google implementerede i 2011, ikke skalerbar, da det kræver, at de offentlige nøgler til hvert enkelt domæne tilføjes i browseren. Der udarbejdes i øjeblikket en skalerbar Public Key Pinning-løsning på baggrund af en foreslået RFC (Request for Comments) i standardiseringsorganisationen IETF (Internet Engineering Task Force).

Forslaget går ud på at definere de offentlige nøgletilknytninger via en http-header fra serveren til browseren. I headeren vil der f.eks. kunne angives en SHA-1 og/eller SHA-256 nøglealgoritme, tilknytningens maksimale varighed, om headeren understøtter underdomæner, hvor nøje tilknytningen skal være osv.



TIP nr. 8 - Brug Perfect Forward Secrecy til at forhindre elektronisk afluring



Hvordan vil I have det med, at jeres nettrafik bliver afluret elektronisk, og at dem, der aflurer trafikken, måske bliver i stand til at dekryptere den? Ikke godt, selvfølgelig. Men ikke desto mindre kan det være den situation, som jeres firma befinder sig i, uden at I overhovedet er klar over faren.

Lad os tage RSA som eksempel. RSA opretter en offentlig og en privat nøgle til at kryptere og kode meddelelser. Men ved fortsat brug af genoprettelige nøgler kan lagrede, krypterede data blive tilgængelige, hvis nøglerne bliver kompromitteret på et tidspunkt. I mange tilfælde kan en hacker med jeres private nøgle og lagret SSL-trafik bruge den private nøgle til at dekryptere alle forhandlede sessionsnøgler ved lagring af SSL-håndtryk og derefter dekryptere alle lagrede sessionsdata ved hjælp af disse sessionsnøgler. Det er svært at have ro i sindet i denne situation. Men der findes en løsning, nemlig "Perfect Forward Secrecy" (PFS).

Med denne løsning er det muligt at oprette, anvende og kassere ikke-genoprettelige, midlertidige sessionsnøgler. Når løsningen implementeres behørigt med Elliptical Curve Cryptography (ECC), se tip nr. 5, er PFS desuden sikrere end RSA-algoritmer og fungerer bedre.

Med PFS er der ingen forbindelse mellem serverens private nøgle og de enkelte sessionsnøgler. Hvis både klient og server understøtter PFS, anvender de en variant af en protokol, der kaldes Diffie-Hellman (opkaldt efter protokollens opfindere), hvor begge parter udveksler vilkårlige numre under sikre forhold og kommer frem til den samme, fælles hemmelighed. Det er en smart algoritme, der forhindrer elektroniske lurere i at finde ud af hemmeligheden, selvom de kan se al nettrafikken.

Se Symantecs infografik for yderligere oplysninger:

[Se infografik](#)



TIP nr. 9 - HTTP Strict Transport Security: jeres sikkerhedsnet



Det er et must, at netsikkerheden altid er i top. Og det betyder nogle gange, at sikkerheden er nødt til at være bedre end standardsikkerhed for at nå op på det ønskede niveau.

Hackere kan bruge man-in-the-middle-angreb i trådløse netværk, som f.eks. omgåelse af SSL, til at opsnappe browseranmodninger til HTTPS-websteder og få returneret anmodede sider over HTTP. Det betyder, at forbindelsen ikke længere er krypteret, og at hackere kan opsnappe information, som ofret indtaster på et angiveligt sikkert websted. Ofret opdager måske aldrig ændringen, fordi han/hun ikke kigger på browserens adresselinje, hver gang der skiftes til en ny side på et websted. Browsers har intet kendskab til, om et websted skal kommunikere sikkert, og derfor bliver brugeren ikke advaret, når et websted indlæses via en ukrypteret forbindelse.

HTTP Strict Transport Security (HSTS) forhindrer dette ved at tillade servere at sende en besked til browseren om, at sådanne forbindelser skal krypteres. Browseren reagerer dernæst på beskeden, så alle websider, som kunden går ind på, bliver krypteret, som de skal, og beskytter jeres firma og jeres kunder mod hackerangreb.

For at aktivere HSTS-beskyttelse skal I angive en single response-header på jeres websteder. Derefter bliver anvisningerne overholdt af browsere, der understøtter HSTS (f.eks. Chromium, Google Chrome, Firefox, Opera og Safari). Efter aktivering tillader HSTS ikke usikker kommunikation med jeres websted. Det sker ved, at alle almindelige tekstbaserede links automatisk konverteres til sikre links.

Internet Explorer understøtter endnu ikke HSTS, men Microsoft har oplyst, at det sker i Internet Explorer 12.

© 2015 Symantec Corporation. Alle rettigheder forbeholdes. Symantec, Symantec-logoet, cirklen med fluebenet og Norton Secured-logoet er varemærker eller registrerede varemærker tilhørende Symantec Corporation eller dets tilknyttede virksomheder i USA og øvrige lande. Øvrige navne kan være varemærker tilhørende de respektive ejere.